(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 388 802 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
11.02.2004 Bulletin 2004/07

(51) Int Cl.[7]: **G06K 9/00**, G06T 3/00, G08B 13/196

(21) Application number: **03016612.8**

(22) Date of filing: **29.07.2003**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(30) Priority: **30.07.2002 JP 2002220655**

(71) Applicant: **Omron Corporation**
Kyoto-shi, Kyoto 600-8530 (JP)

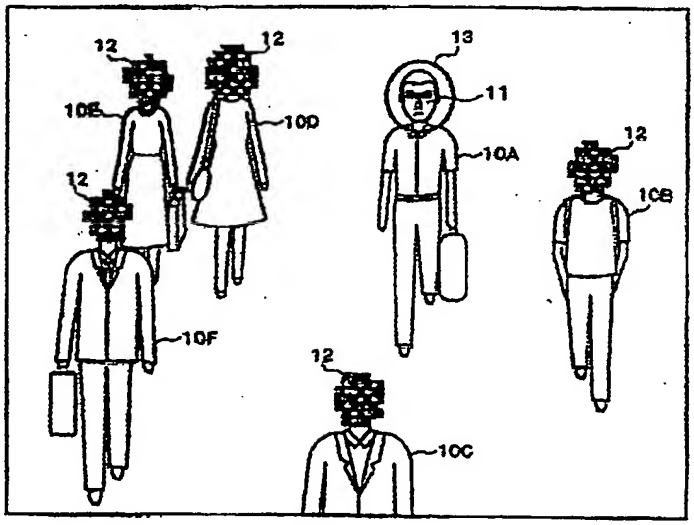
(72) Inventor: **Takenaka, Hideki, Omron Corp.**
801 Minamifudodo-cho
Kyoto-shi, Kyoto 600-8530 (JP)

(74) Representative: **Käck, Jürgen**
Kahler Käck Mollekopf
Patentanwälte
Vorderer Anger 239
86899 Landsberg (DE)

(54) Face identification device and face identification method

(57) The present invention is to protect the right of portrait or privacy of people (10B to 10F) other than a specific person (10A), and to enable easy recognition of information other than the face (11) of the specific person (10A) and the situation around the specific person (10A). Images videotaped by the surveillance cameras (1) are captured in the computer (3), face images are detected therefrom, and the detected face images are compared with the face image of a specific person (10A) registered in the storage device (5). As the results of the comparison, when these face images do not match with each other, a mosaic process (12) is applied exclusively to the detected face images to protect the privacy of the people (10B to 10F) other than the specific person (10A), whereas the mosaic process (12) is not applied to the parts other than the faces, such as dress and baggage, thereby keeping them as they are. When these face images match with each other, the face image of the specific person (10A) is not applied with the mosaic process (12), thereby keeping his or her face (11) and remaining parts as they are.

Fig. 5



EP 1 388 802 A2

Description

BACKGROUND OF THE INVENTION

Technical Field

[0001] The present invention relates to a face identification technique which detects human faces from images taken by a camera and compares themwith a previously registered face, thereby detecting a specific person.

Related Background Art

[0002] In order to search for a specific person like a criminal on the wanted list, such a system is available that videotapes an unspecified number of the general public and records their images by installing surveillance cameras in airports, stations, shopping centers, busy streets, and the like. In this system, videotaped images are recorded as they are or face images are exclusively recorded by being extracted from the videotaped images. In these methods, there is a problem that face images of the people other than the specific person are also recorded, failing to protect their rights of portrait or privacy.

[0003] Therefore, there is a system now available, according to which the face image of a person videotaped by a surveillance camera is compared with the face image of the specific person registered: the face image of a videotaped person is recorded if these face images match with each other, whereas when these face images do not match with each other, the face image of the videotaped person is abandoned. In this system, out of the face images videotaped, those which do to match with the face image of the registered specific person are not kept, thereby securing protection of their privacy.

[0004] However, in the above-described system, what is recorded is only the face image matching with the face image of the specific person, and other useful information including the dress and baggage of the specific person and the situation around him or her are lost. As a result, when there is a match and a responsible official rushes to the display monitor by a report or when recorded images are confirmed later, the absence of information other than his or her face makes it difficult to search for the specific person.

[0005] On the other hand, in order to protect individuals' privacy, there is an approach of applying a mosaic process on face images as described in Japanese Laid-Open Patent Application No. 2001-86407. However, in this patent application, skin color is detected from videotaped human images and a mosaic process is automatically applied to face images, which forces all face images videotaped to be applied with a mosaic process, thereby making it impossible to apply a mosaic process to the face images excluding the face image of the specific person.

[0006] Japanese Laid-Open Patent Application No. 2000-216 also discloses privacy protection measures by applying a mosaic process to human body images. However, when the technique of this patent application is used to protect the privacy of the people other than the specific person, it is difficult to check the situation around the specific person, because the whole image of the specific person is applied with the mosaic process.

DISCLOSURE OF THE INVENTION

[0007] The present invention, which is intended to solve the aforementioned problems, has the object of facilitating confirmation of information other than the face of a specific person and situation around the specific person, while protecting the right of portrait or privacy of the people other than the specific person.

[0008] The face identification device of the present invention comprises: detection means for detecting face images from human body images taken by a camera; storage means in which a face image of a specific person is previously stored; determination means for determining whether a face image detected by the detection means matches with the face image stored in the storage means by comparing both face images; and abstraction means for applying an abstraction process to a predetermined face image out of the face images detected by the detection means in order to make the predetermined face image unrecognizable. The abstraction means applies the abstraction process exclusively to a detected face image when the determination means determines that both face images do not match with each other. On the other hand, the abstraction means does not apply the abstraction process to a detected face image when the determination means determines that both face images match with each other.

[0009] The face identification method of the present invention comprises the steps of: detecting face images from human body images taken by a camera; determining whether a detected face image matches with the face image previously stored by comparing both face images; applying an abstraction process exclusively to a detected face image in order to make the detected face image unrecognizable, when it is determined that both face images do not match with each other; and not applying the abstraction process to the detected face image when it is determined that both face images match with each other.

[0010] The term "match" referred to in the above description means not only a complete match between a detected face image and the face image previously stored, but also a high degree of resemblance between these face images.

[0011] According to the present invention, when a detected face image and the registered face image do not match with each other, that is, when the detected face does not belong to the specific person, an abstraction

process is applied on the face image in order to protect the right of portrait or privacy of the people other than the specific person. Furthermore, the abstraction process is applied only to the face images of the people, keeping images other than their faces, such as their dress and baggage. On the other hand, when a detected face image and the registered face image match with each other, that is, when the detected face belongs to the specific person, both the face image and images including the dress and baggage of the specific person are kept without being applied with the abstraction process. Thus keeping the images for the dress and baggage of a specific person and of the other people as they are can facilitate the search for the specific person by using these images as an important clue.

[0012] A typical example of the abstraction process in the present invention is a mosaic process. The use of the well-known mosaic process can abstract face images easily. Besides the mosaic process, various other methods are available for abstraction, such as blurring or filling in face image portions.

[0013] In the present invention, when it is determined that a detected face image matches with the stored face image, a marker is applied to the detected face image portion instead of applying an abstraction process thereto. The application of a marker makes a specific person distinguishable at a glance.

[0014] In the present invention, when it is determined that a detected face image matches with the stored face image, the image of the specific person applied with the abstraction process neither to his or her face nor remaining parts and the images of the other people applied with the abstraction process exclusively to their faces are displayed. At the same time, a warning is outputted. This system realizes a quick response because the warning is outputted at the time of the detection of a specific person. Concerning a specific person, the videotaped image is displayed as it is, and as for the people other than the specific person, the abstraction process is applied to their faces to protect their privacy while the images of their dress and baggage are displayed as they are. This makes it possible to obtain useful information about the specific person and the situation around him or her, thereby facilitating the search for the specific person.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015]

Fig. 1 shows a block diagram of the face identification system to which the present invention is applied.

Fig. 2 shows a flowchart depicting the procedure for registering face images.

Fig. 3 shows a flowchart depicting the procedure of the face identification method of the present invention.

Fig. 4 shows a flowchart depicting a specific procedure of identification.

Fig . 5 shows an image example to which mosaic process has been applied.

Fig. 6 shows a flowchart depicting the identification procedure in the case where a face image is registered afterwards.

Fig. 7 shows a flowchart depicting another embodiment of the face identification method.

Fig. 8 shows a flowchart depicting the identification procedure in the case where a face image is registered afterwards in another embodiment.

Fig. 9 shows a block diagram showing another embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0016] Fig. 1 shows a block diagram of the face identification system to which the present invention is applied. In the drawing, the face identification system is composed of surveillance cameras 1 for videotaping the images of people, and the face identification device 2 of the present invention for identifying face images of the people videotaped by the surveillance cameras 1. Aplural number of the surveillance cameras 1 are installed in airports, stations, shopping centers, busy streets, and other places where a number of people gather, and each of the cameras 1 is connected with the face identification device 2 installed in a monitor center or the like.

[0017] In the face identification device 2, reference numeral 3 is a computer for face identification; reference numeral 4 is an identification results output device for outputting the results of face identification by the computer 3; and reference numeral 5 is a storage device which previously stores the face image data of a specific person (e.g., a suspect on the wanted list). Reference numerals 6 and 7 are image input devices for registering a face image to the storage device 5: reference numeral 6 is a scanner and reference numeral 7 is a digital camera. The computer 3 includes detection means for detecting face images from images of people videotaped by the surveillance cameras 1; determination means for determining the presence or absence of a match between a detected face image and the face image stored in the storage device 5 by comparing them; and abstraction means for applying an abstraction process to a predetermined face image out of the detected face images so as to make the face unrecognizable. The identification results output device 4 is composed of a display monitor for displaying identification results, a printer for printing identification results, and other output devices. The storage device 5 can be a hard disk or the like, which composes the storage means of the present invention. Besides a hard disk, an optical disk can be used as the storage means.

[0018] Operation of the face identification system having the above-explained structure will be described as follows. In this system, the face image of a specific

person is previously registered in the storage device 5. Fig. 2 shows a flowchart depicting the procedure of face image registration, which is executed by the computer 3. At first, an image including the face of a specific person to be registered is captured into the computer 3 from the scanner 6 or the digital camera 7 (Step S1). Next, the face to be registered is detected from the captured image (Step S2). This face detection can be done by using a well-known approach, such as skin color detection, abstraction of difference with a background image, or abstraction of face likelihood from pattern matching. After the face detection, featuring points such as eyes, nose, mouth, and ears are detected from the face image (Step S3) , and the amount of feature about the shape and position of each detected featuring point is extracted (Step S4). This abstraction of feature amount also can be done by using a well-known approach, such as extraction of the amount of feature from gray-scale images including eyes, nose, mouth, and ears by template matching. The amount of feature extracted is stored and registered in the storage device 5 as face image data (Step S5).

[0019] Fig. 3 shows a flowchart depicting the procedure of the face identification method of the present invention, the procedure being executed by the computer 3. In the computer 3 , images videotaped by the surveillance cameras 1 are captured as still images at the interval of e.g. one second (Step S11), and human faces are detected from the captured images (Step S12). If there is no face detected (Step S13:NO), the process goes back to Step S11 and captures images in the next timing. If a face is detected (Step S13:YES), the detected face image is compared with the face image previously registered in the storage device 5 (Step S14) so as to determine whether or not these face images match with each other (Step S15).

[0020] Fig. 4 shows a flowchart depicting the specific procedure of the comparison in Step S14 . In the comparison, featuring points (eyes, nose, mouth, and the like) are detected from the detected face image (Step S31), and the amount of feature about the shape and position of each detected featuring point is extracted (Step S32). The extracted amount of feature is compared with the amount of feature of the face registered in the storage device 5 (Step S33). Based on the comparison results, it is determined whether these face images match with each other or not at Step S15 shown in Fig. 3. The term "match" referred to in this case means not only a complete match, but also a high degree of resemblance between these face images. To be more specific, the degree of resemblance is calculated from the amount of feature of each face image, and is compared with a predetermined threshold value. When the degree is equal to or over the threshold value, it is determined as a match.

[0021] As the results of the determination at Step S15, when a detected face image and the registered face image do not match with each other (Step S15:NO), the detected face image does not belong to the specific person registered. Therefore, the mosaic process is applied to the detected face image portion (Step S16). Fig. 5 shows an example of images to which the mosaic process has been applied: the mosaic process 12 is applied to each face image of the persons 10B to 10F except the specific person so as to abstract their faces unrecognizably. The mosaic process 12 is applied exclusively to the face image portions, keeping dress and baggage portions unprocessed.

[0022] On the other hand, when a detected face image matches with the registered face image (Step S15: YES), it means that the detected face image belongs to the registered specific person, so a marker is applied to the detected face image portion instead of applying the mosaic process thereto (Step S17). In Fig. 5, the person 10A is the specific person, and the mosaic process 12 is not applied to the face image portion of the specific person 10A, thereby keeping the face 11 the same as when it is videotaped by the surveillance cameras 1. The face 11 is enclosed by the marker 13 to make the specific person distinguishable at a glance. The mosaic process 12 is not applied to the dress or baggage of the specific person 10A. In other words, concerning the specific person 10A, the image videotaped by the surveillance cameras 1 appears as it is.

[0023] After the process in Step S17, the identification results output device 4 displays, with a warning, the images shown in Fig. 5 including the image of the specific person 10A whose face and remaining parts are not applied with the mosaic process 12, and the images of the persons 10B to 10F whose faces are exclusively applied with the mosaic process (Step S18). This warning is displayed as a message including the name of the specific person, the time and date of the image videotaped, and the place videotaped. Furthermore, an alarm is issued as necessary with the display in order to draw the responsible official's attention. This enables the official to prepare the deployment of members for the search for the specific person.

[0024] Since the faces of the people other than the specific person 10A are applied with the mosaic process 12 as shown in Fig. 5, when the images are displayed on the display monitor, there is no fear of violating their rights of portrait or privacy. Furthermore, the mosaic process 12 is applied exclusively to their faces, keeping the remaining parts unprocessed, which enables easy recognition of the dress and baggage of the people around the specific person 10A. On the other hand, concerning the specific person 10A, the videotaped image of the whole body appears as it is, making it possible to confirm his dress and baggage in addition to his face. Thus, the mosaic process 12 is applied exclusively to face portions which raise the issue of privacy, and the remaining parts are kept the same as when they are videotaped, thereby facilitating the search for the specific person 10A by using the dress and baggage as a useful clue.

[0025] After Steps S16 to S18 are executed, it is determined whether matching is done for all the detected faces (Step S19). When there is still a face to be checked (519:NO) the process goes back to Step S14 to check the next face. When all the detected faces have been checked (S19:YES) , the image to which the procedure of Steps S16 and S17 has been applied is recorded to the storage device 5 (Step S20). Later, the process goes back to Step S11, and videotaped images are captured from the surveillance cameras 1 again in the next timing (in one second in this case) . Hereafter, the procedure in Steps S12 to S20 is repeated.

[0026] The above example describes the case where images videotaped by the surveillance cameras 1 are captured as still images at the interval of one second; however, it is also possible to adopt a system which detects human faces from motion images videotaped by the surveillance cameras 1 and checks the faces while automatically chasing them. In this system, there is no need for the repeated recording of the image of the same person, which can reduce the amount of image data to be recorded in the storage device 5, thereby enabling miniaturization of the storage device 5.

[0027] Images stored in the storage device 5 can be outputted by being displayed or printed by the identification results output device 4 later at any point in time. In this case, too, the privacy of the people other than the specific person 10A is protected by applying the mosaic process to their faces, whereas the images for the dress and baggage including those of the specific person are stored as they are. This information can be used as a clue to facilitate the search for the specific person 10A.

[0028] In the aforementioned embodiment, the face image of a specific person is previously registered, and face images videotaped by surveillance cameras are compared with the registered face image so as to detect the specific person; however, it is also possible to detect a specific person registered afterwards by using images stored in the storage device 5. This system enables the detection of people whom the police has been requested to find or stray children.

[0029] Fig. 6 shows a flowchart depicting the procedure of identification in the case of registering afterwards as described above, the procedure being executed by the computer 3 . At first, images stored in the storage device 5 are captured by the computer 3 (Step S41). The images stored in the storage device 5 are unrecognizable because of the above-described mosaic process, so it is necessary to reconstruct the original images for comparison. Therefore, the mosaic process is cleared to reconstruct the original images (Step S42). After the reconstruction of the original images, faces are detected from the reconstructed images (Step S43) . If no face is detected from the reconstructed images (Step S44:NO), the process goes back to Step S41 to capture recorded images. On the other hand, if faces are detected from the reconstructed images (Step S44:YES), detected face images are compared with the face image which is registered afterwards (Step S45). The face image registered afterwards is taken by the scanner 6 or the digital camera 7 and recorded to the storage device 5 in the same manner as the previously registered case.

[0030] If the comparison results in Step S45 indicate that a recorded image face does not match with the face registered afterwards (Step S46:NO), it is determined whether all faces detected from the recorded images have been checked or not (Step S47). When there is a face left unchecked (Step S47:NO), the process goes back to Step S45 to check the next face. When all faces have been checked (Step S47:YES), it is determined whether all the recorded images have been checked or not (Step S48). If all recorded images are not checked (Step S48:NO), the process goes back to Step S41 to capture the next recorded image from the storage device 5 and the aforementioned procedure is repeated. When the comparison for all recorded images is complete (Step 548:YES), the absence of the face image matching with the face image registered afterwards is reported by being displayed on the display monitor of the identification results output device 4 (Step S49).

[0031] On the other hand, in Step S46, if a recorded face image matches with the face registered afterwards (Step S46:YES), the reconstructed original image is outputted to the identification results output device 4 and shown on the display monitor (Step S50). And it is reported by being shown on the display monitor that there is a recorded face image which matches with the face registered afterwards (Step S51).

[0032] In the comparison in the above-described case where a face image is registered afterwards, it is preferable in terms of security that the process for reconstructing original images by clearing the mosaic process applied to images stored in the storage device 5 can be done exclusively by an authorized person (e.g., system administrator). Figs. 7 and 8 show flowcharts depicting the embodiment of this case.

[0033] Fig. 7 shows a flowchart corresponding to the flowchart shown in Fig. 3, so the same steps as those in Fig. 3 are referred to with the same symbols. The procedure in Steps S11 to S19 is the same as in Fig.3, so its explanation is omitted. When all faces have been checked in Step S19 (Step S19:YES), the face image of a recorder who records images is captured (Step S20a); the captured face image of the recorder is embedded as a "digital watermark" in the images processed in Steps S16 and S17; and the images with the "digital watermark" are stored in the storage device 5 (Step S20b) . The term "recorder" used in this case can be a system administrator, and the face image of the recorder which is captured in Step S20a is previously taken by the scanner 6 or the digital camera 7 and stored in the storage device 5.

[0034] The following is a description on the procedure for reconstructing original images. Fig. 8 shows a flowchart corresponding to the flowchart of Fig. 6, so the same steps as those in Fig. 6 are referred to with the

same symbols. First, images stored in the storage device 5 are captured in the computer 3 (Step S41). Next, the face image of the operator who performs a reconstructing operation of images is captured (Step S41a). The face image of this operator is taken by the scanner 6 or the digital camera 7 at this point in time. Then, it is determined whether the face image data captured in Step S41a matches with the data of "digital watermark" embedded in the images captured in Step S41 or not (Step S41b). If these pieces of data do not match with each other (Step S41b:NO), it is determined that the operator who is going to perform the reconstructing operation is not the above-mentioned recorder (systemadministrator), and the process is terminated. On the other hand, when these pieces of data match with each other (Step S41b:YES), it is determined that the operator and the recorder (system administrator) are the same person, and the mosaic process is cleared to reconstruct the original images (Step S42). Since the procedure from Step S42 onward is equal to the procedure in Fig. 6, the explanation will be omitted.

[0035] As described hereinbefore, using the face image of the recorder as a "digital watermark" makes it possible to authorize only the recorder to perform reconstruction and to prohibit an unauthorized third party from clearing a mosaic process to reconstruct original images, thereby securing the security.

[0036] The present invention can adopt various other embodiments besides the embodiment described above. For example, in the above embodiment, a mosaic process is taken as an example of the abstraction process to be applied to face images; however, it is also possible to apply a process to blur face image portions, instead of applying the mosaic process. Alternatively, face image portions can be filled in black or white, instead of being applied with the mosaic process or the blurring process.

[0037] In the above embodiment, images which are videotaped by the surveillance cameras 1 and applied with a mosaic process or a marker are stored in the storage device 5; however, the images can be merely displayed on the display monitor of the identification results output device 4. In this case, there is no need for storage to the storage device 5.

[0038] In the above embodiment, face images which are registered either previously or afterwards are stored in the storage device 5, and images which are videotaped by the surveillance cameras 1 and applied with a mosaic process or a marker are also stored in the same storage device 5. Alternatively, as shown in Fig. 9, a special image storage device 8 can be provided in addition to the storage device 5 so that face images to be registered can be stored in the storage device 5 whereas images videotaped by the surveillance cameras 1 can be stored in the image storage device 8. The image storage device 8 can be composed of any kind of device dealing with recording media such as a video tape recorder, a DVD (Digital Versatile Disk) recorder, or a hard disk recorder. In that case, faces other than the face of the specific person are applied with an abstraction process, so there is no fear of violating their rights of portrait or privacy during reproduction.

[0039] According to the present invention, an abstraction process is applied exclusively to the face images of the people other than a specific person, thereby protecting their rights of portrait or privacy, whereas the images for the dress and baggage of the specific person and the other people are kept as they are. This information can be used as a clue to facilitate the search for the specific person.

Claims

1. A face identification device (2) comprising:

   detection means for detecting face images from human body images taken by a camera;
   storage means in which a face image of a specific person (10A) is previously stored;
   determination means for determining whether a face image detected by said detection means matches with the face image stored in said storage means by comparing both face images; and
   abstraction means for applying an abstraction process to a predetermined face image out of the face images detected by said detection means in order to make the predetermined face image unrecognizable,
   said abstraction means applying the abstraction process exclusively to a detected face image when said determination means determines that both face images do not match with each other, and not applying the abstraction process to a detected face image when said determination means determines that both face images match with each other.

2. The face identification device (2) according to claim 1, wherein said abstraction process is a mosaic process (12) for making a face image portion mosaic.

3. The face identification device (2) according to claim 1 or 2, wherein when said determination means determines that both face images match with each other, a detected face image is not applied with the abstraction process and is applied with a marker (13).

4. The face identification device (2) according to any one of claims 1 to 3 , wherein when a face image detected by said detection means is determined to match with the face image stored in said storage means, the image of the specific person (10A)

which is not applied with the abstraction process on the face (11) and remaining parts thereof and the images of people (10B to 10F) other than the specific person (10A) which are applied with the abstraction process exclusively on the faces thereof are displayed, and a warning is also outputted.

5. A face identification method comprising the steps of:

detecting face images from human body images taken by a camera;
determining whether a detected face image matches with the face image previously stored by comparing both face images;
applying an abstraction process exclusively to a detected face image in order to make the detected face image unrecognizable, when it is determined that both face images do not match with each other; and
not applying the abstraction process to the detected face image when it is determined that both face images match with each other.

Fig. 1

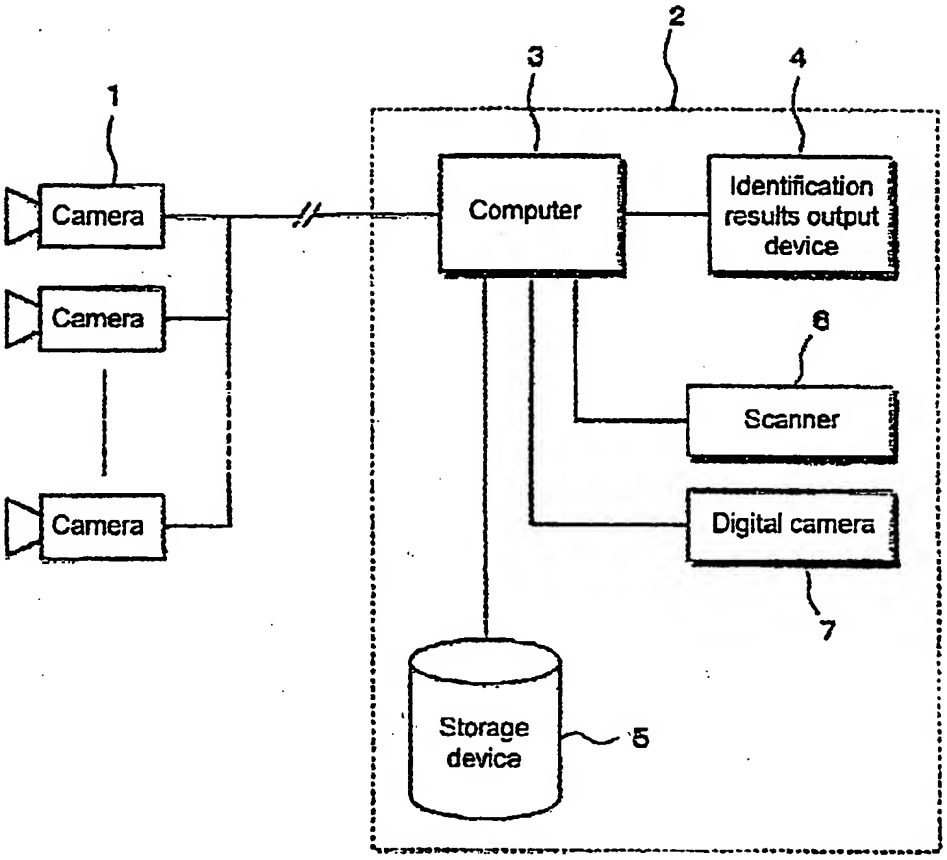

1
2
3
4
Camera
Camera
Camera
Computer
Identification results output device
6
Scanner
Digital camera
7
Storage device
5

Fig. 2

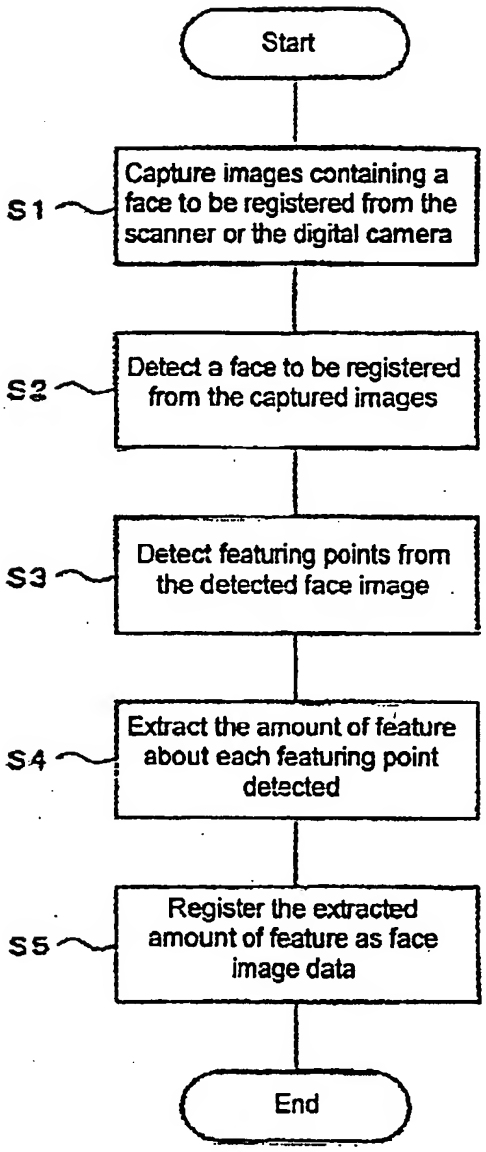

Start
S1
Capture images containing a face to be registered from the scanner or the digital camera
S2
Detect a face to be registered from the captured images
S3
Detect featuring points from the detected face image
S4
Extract the amount of feature about each featuring point detected
S5
Register the extracted amount of feature as face image data
End

Fig. 3

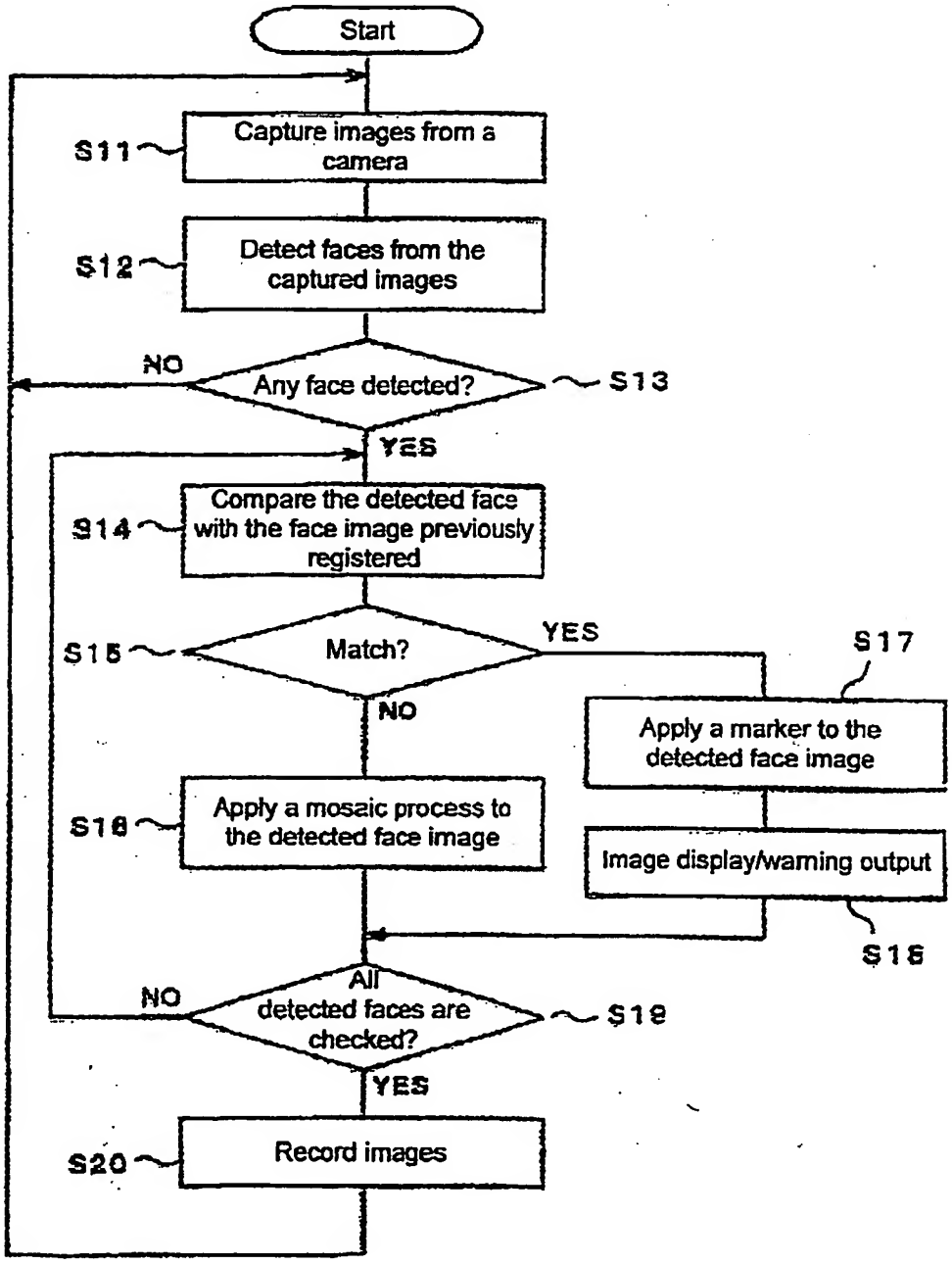

Start
S11
Capture images from a camera
S12
Detect faces from the captured images
NO
Any face detected?
S13
YES
S14
Compare the detected face with the face image previously registered
S15
Match?
YES
S17
NO
Apply a marker to the detected face image
S16
Apply a mosaic process to the detected face image
Image display/warning output
S18
NO
All detected faces are checked?
S19
YES
S20
Record images

Fig. 4

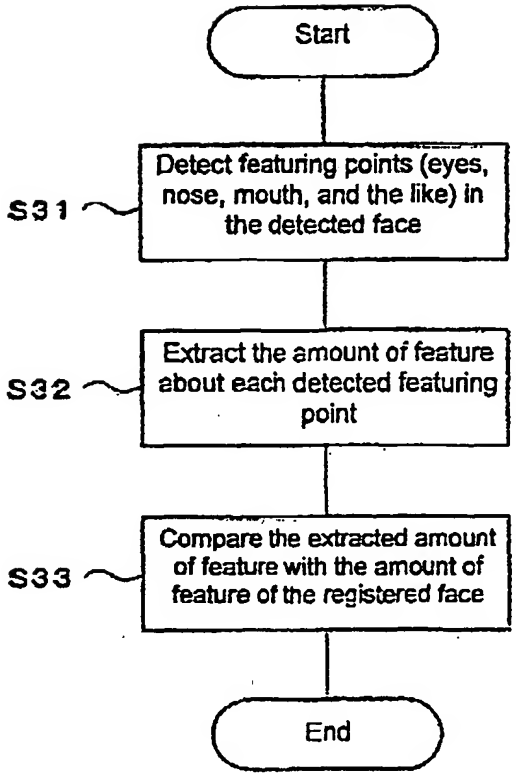

Start
S31
Detect featuring points (eyes, nose, mouth, and the like) in the detected face
S32
Extract the amount of feature about each detected featuring point
S33
Compare the extracted amount of feature with the amount of feature of the registered face
End

Fig. 5

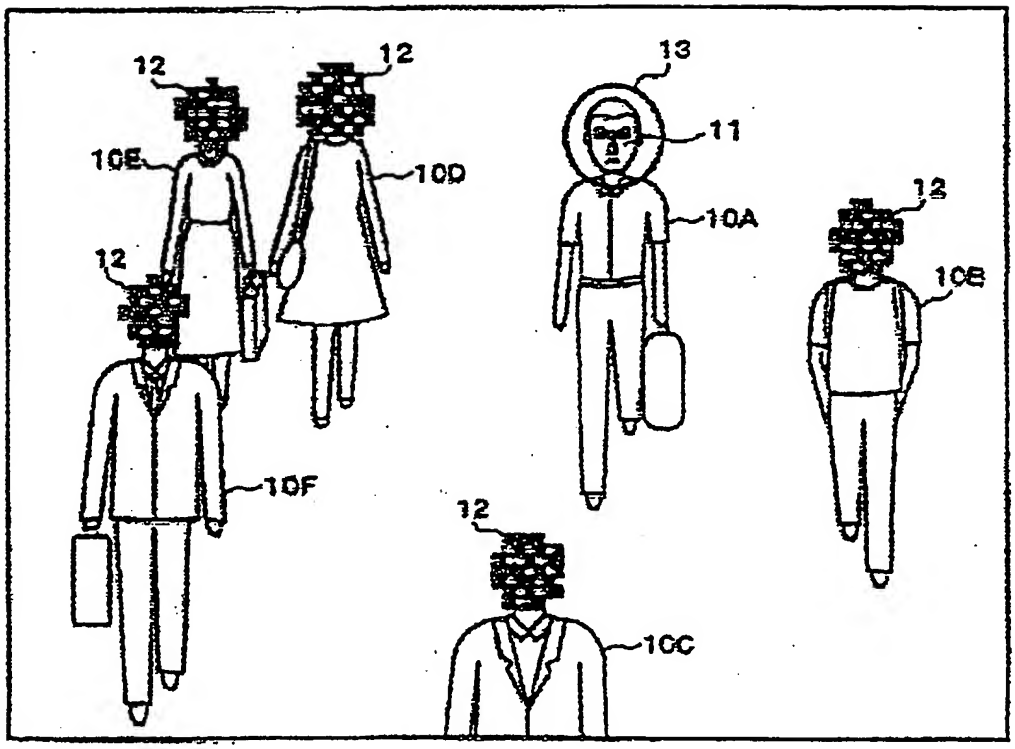


Fig. 6

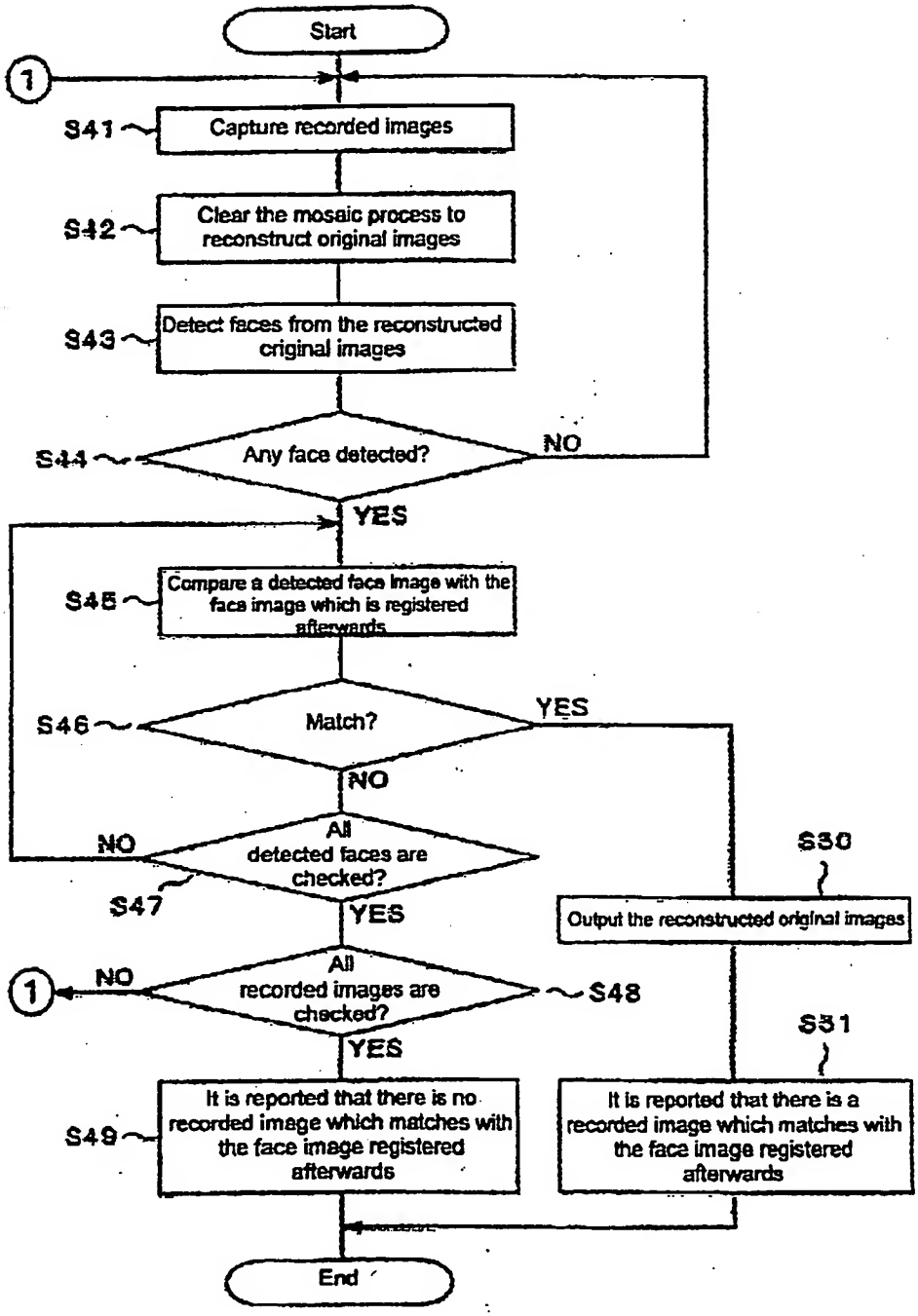

Start
1
S41
Capture recorded images
S42
Clear the mosaic process to reconstruct original images
S43
Detect faces from the reconstructed original images
S44
Any face detected?
NO
YES
S45
Compare a detected face image with the face image which is registered afterwards
S46
Match?
YES
NO
NO
All detected faces are checked?
S47
YES
S50
Output the reconstructed original images
1
NO
All recorded images are checked?
S48
YES
S51
S49
It is reported that there is no recorded image which matches with the face image registered afterwards
It is reported that there is a recorded image which matches with the face image registered afterwards
End

Fig. 7

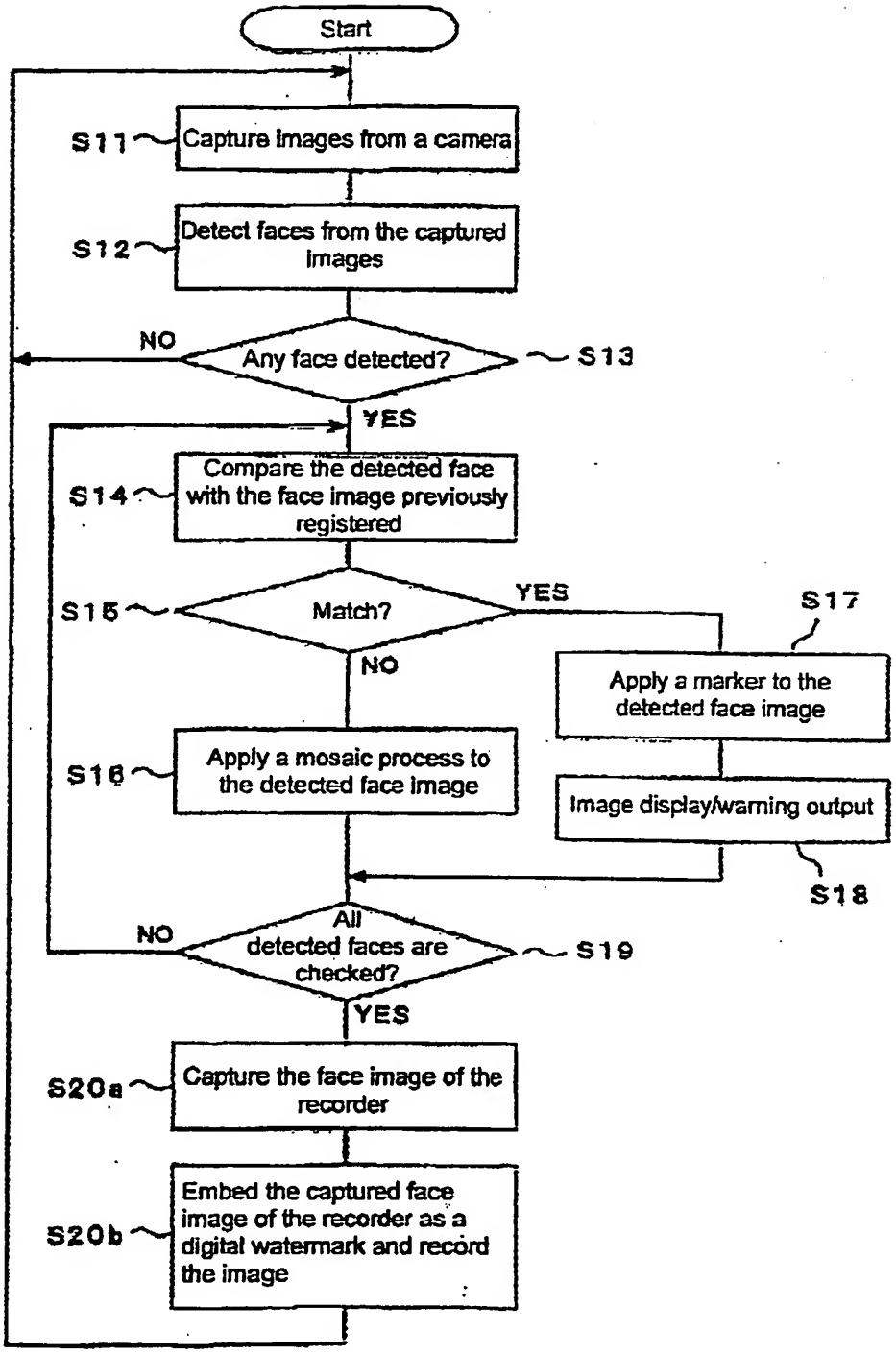

Start
S11
Capture images from a camera
S12
Detect faces from the captured images
NO
Any face detected?
S13
YES
S14
Compare the detected face with the face image previously registered
S15
Match?
YES
S17
NO
Apply a marker to the detected face image
S16
Apply a mosaic process to the detected face image
Image display/warning output
S18
NO
All detected faces are checked?
S19
YES
S20a
Capture the face image of the recorder
S20b
Embed the captured face image of the recorder as a digital watermark and record the image

Fig. 8

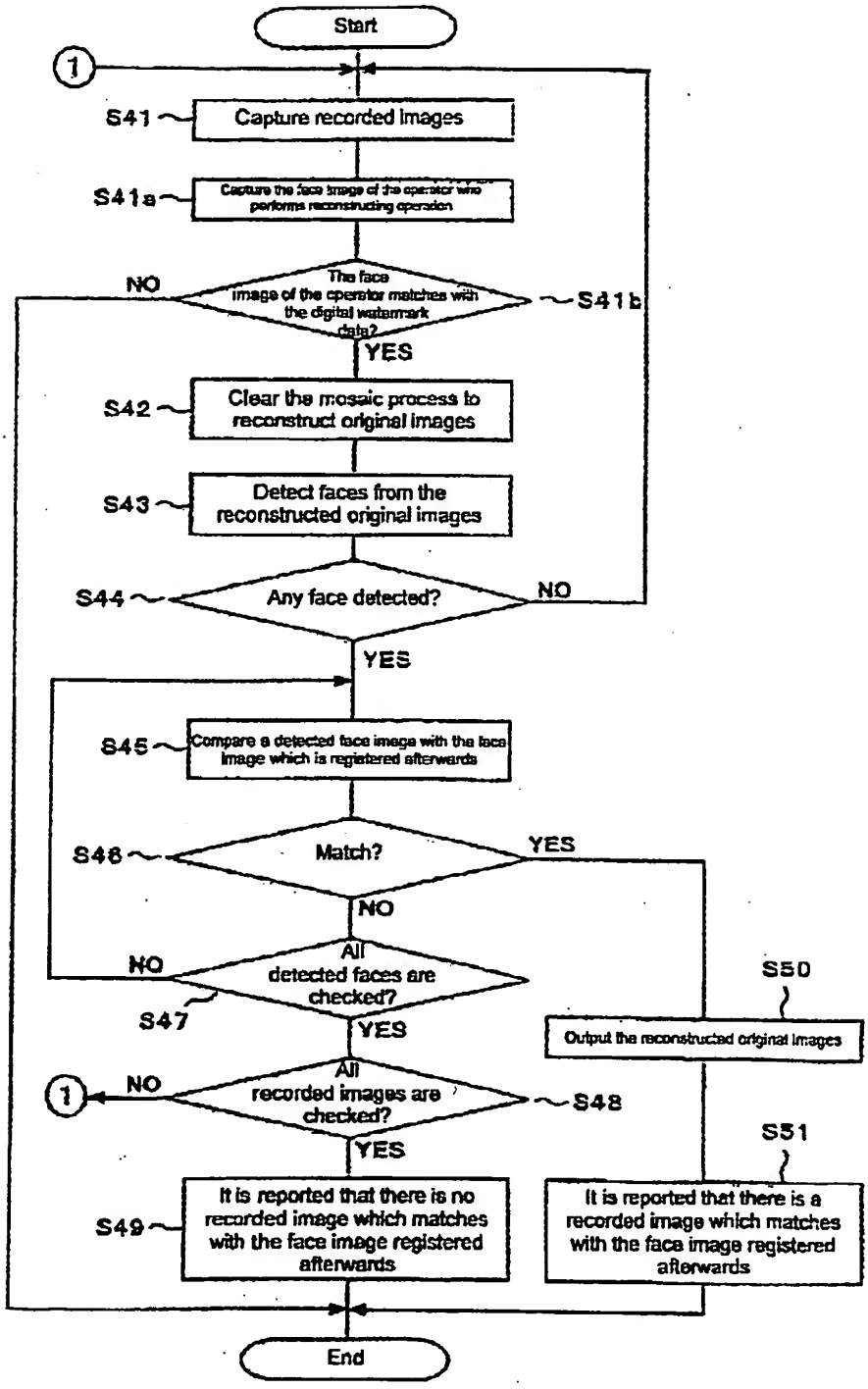
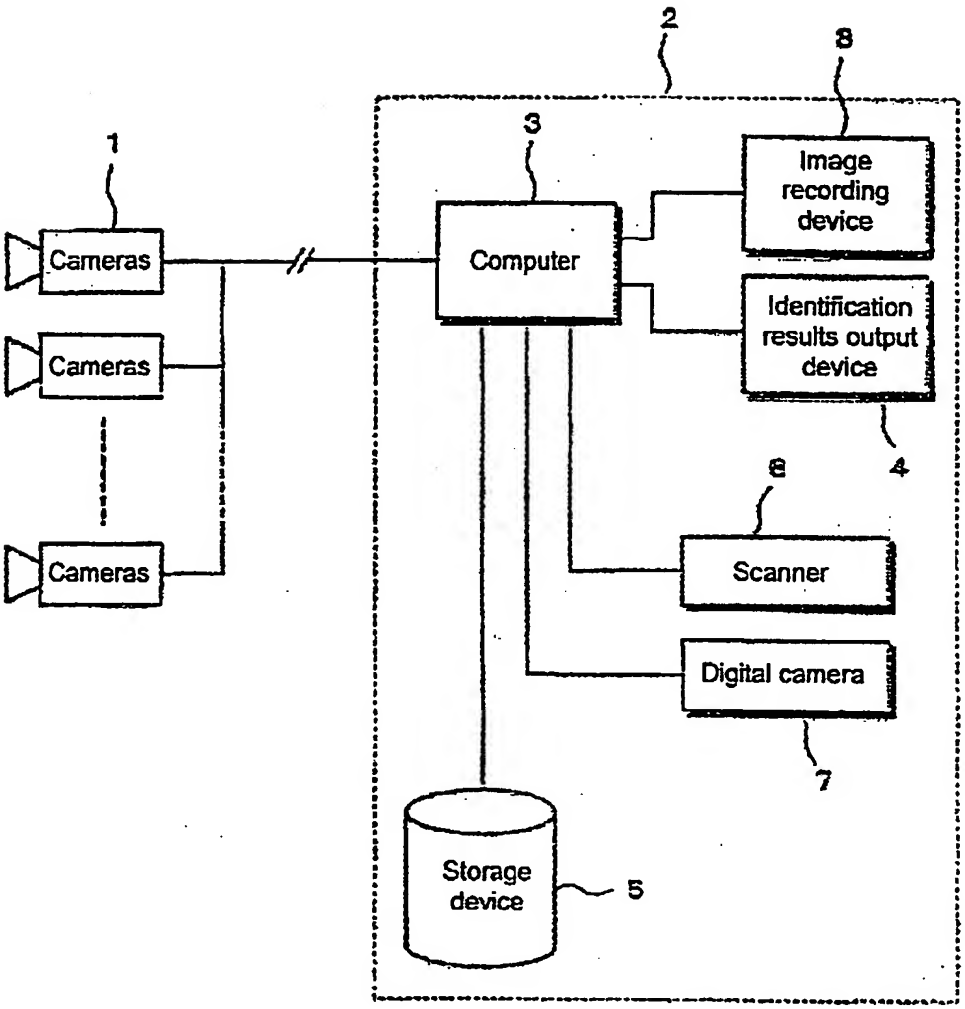

Start
1
S41
Capture recorded images
S41a
Capture the face image of the operator who performs reconstructing operation
NO
The face image of the operator matches with the digital watermark data?
S41b
YES
S42
Clear the mosaic process to reconstruct original images
S43
Detect faces from the reconstructed original images
S44
Any face detected?
NO
YES
S45
Compare a detected face image with the face image which is registered afterwards
S46
Match?
YES
NO
NO
All detected faces are checked?
S47
YES
S50
Output the reconstructed original images
1
NO
All recorded images are checked?
S48
YES
S51
S49
It is reported that there is no recorded image which matches with the face image registered afterwards
It is reported that there is a recorded image which matches with the face image registered afterwards
End

Fig. 9


2
8
1
3
Image recording device
Cameras
Computer
Identification results output device
Cameras
4
6
Scanner
Cameras
Digital camera
7
Storage device
5